IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re: Clearview AI, Inc. Consumer Privacy Litigation,	Case No. 1:21-cv-00135 Judge Sharon Johnson Coleman Magistrate Judge Maria Valdez

BRIEF OF AMICUS ELECTRONIC FRONTIER FOUNDATION IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

Adam Schwartz
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Tel.: (415) 436-9333
Fax: (415) 546-9993
adam@eff.org
jlynch@eff.org

Attorneys for Amicus Curiae
Electronic Frontier Foundation

July 9, 2021

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases

STATEMENT OF INTEREST

The Electronic Frontier Foundation (EFF) works to ensure that technology supports freedom, justice, and innovation for all the people of the world. EFF is a non-profit with more than 30,000 members. EFF advocates in courts and legislatures for free speech and biometric privacy. EFF has appeared as an amicus concerning Illinois' Biometric Information Privacy Act (BIPA). *Rosenbach v. Six Flags Entmt. Corp.*, 432 Ill. Dec. 654 (2019); *Patel v. Facebook*, 932 F.3d 1264 (9th Cir. 2019). EFF's Illinois members enjoy BIPA's protections.

INTRODUCTION

Clearview AI extracts faceprints from billions of photos of people's faces. The company calls them "facial vectors," and says they are "numerical hashes generated by a machine-learning algorithm which analyzes faces." Dkt. No. 88 (Def. Br.) at p. 10. Clearview had no reason to think that any particular person in these photos would engage in a matter of public concern. Rather, its sole purpose was to sell law enforcement agencies the service of identifying unknown people in probe photographs. It extracted these faceprints without first getting permission from the people in the photographs. Clearview thereby violated BIPA, which requires a private entity to obtain a person's opt-in consent before collecting their biometrics. 740 ILCS 14/15(b).

This BIPA requirement does not violate the First Amendment as applied to Clearview's faceprinting. The company's contrary arguments lack merit. *See* Def. Br. at pp. 9-17.

This faceprinting enjoys at least some level of First Amendment protection, because it is collection and creation of information in order to later express information. *Infra* Part I. The test is intermediate review, because the information Clearview collects and shares by faceprinting is not a matter of public concern, and Clearview's interest is solely economic. This test requires a close fit between a speech limit and a substantial government interest. *Infra* Part II.

The application of BIPA to Clearview easily passes this test. Everywhere we go, we display a unique and indelible marker that can be seen from a distance: our own faces. So corporations can use face surveillance technology (coupled with the ubiquity of digital cameras) to track where we go, who we are with, and what we are doing. Illinois has substantial interests in protecting privacy, and the free speech and information security that depend on privacy, from the special hazards of faceprinting. *Infra* Part III. BIPA's requirement of opt-in consent to collect faceprints is narrowly drawn to these interests. Illinois has placed control over whether a business may extract a faceprint from a person exactly where it belongs: with that person. *Infra* Part IV. Thus, the First Amendment does not protect Clearview's faceprinting from BIPA.

ARGUMENT

I. Faceprinting enjoys at least some First Amendment protection.

The First Amendment protects not just expression, but also the necessary predicates that enable expression, including the collection and creation of information. Faceprinting involves both the collection of information (*i.e.*, measurements of a face) and the creation of information (*i.e.*, representations of a face). Faceprinting will often be the necessary predicate to expression about the person behind the face. For example, a journalist or police reform advocate might use faceprinting to publicly name the unidentified police officer depicted in a video using excessive force. Or here, Clearview uses faceprinting to sell its law enforcement clients the service of providing information about an unidentified suspect in a police photo. *Infra* Part I(A).

First Amendment protection of faceprinting is not diminished by the use of computer code to collect information about faces, or the use of mathematical representations of these faces. Computer code consistently receives First Amendment protection despite its functional aspects because it is a means of exchanging ideas and information. *Infra* Part I(B).

However, the First Amendment does not always preclude regulation of faceprinting, and does not necessarily require that such regulations survive the strictest judicial review. In this case, the correct First Amendment test is intermediate review, *infra* Part II, and the application of BIPA to Clearview's faceprinting passes this test, *infra* Parts III-IV.

A. The First Amendment protects the necessary predicates to expression.

The First Amendment protects the right to collect information, as a required step in the process of expression. For example, when ruling against the removal of books from a library, the U.S. Supreme Court held that "the right to receive ideas is a necessary predicate to the *recipient's* meaningful exercise of his own rights of speech, press, and political freedom." *Board of Educ. v. Pico*, 457 U.S. 853, 867 (1982). Likewise, when protecting public access to criminal trials, the Court held: "The explicit, guaranteed rights to speak and to publish concerning what takes place at a trial would lose much meaning if access to observe the trial could, as it was here, be foreclosed arbitrarily." *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555, 576-77 (1980).

For the same reason, the First Amendment also protects the right to create information. As the Court explained when striking down a restraint on video games: "Whether government regulation applies to creating, distributing, or consuming speech makes no difference." *Brown v. Entmt. Merchants Assn.*, 564 U.S. 786, 792 n.1 (2011). Otherwise, government could evade the First Amendment's protection of speech by moving upstream and suppressing the creation of speech. *See Citizens United v. FEC*, 558 U.S. 310, 336 (2010) ("Laws enacted to control or suppress speech may operate at different points in the speech process."). *See also Minneapolis Star & Tribune Co. v. Minn. Commr. Of Revenue*, 460 U.S. 575, 582 (1983) (striking down a tax on ink and paper). As the Ninth Circuit explained when striking down a ban on tattoo parlors:

> "[N]either the Supreme Court nor our court has ever drawn a distinction between the process of creating a form of pure speech (such as writing or painting) and the product of these processes (the essay or the artwork) in terms of the First Amendment protection afforded. Although writing and painting can be reduced to their constituent acts, and thus described as conduct, we have not attempted to disconnect the end product from the act of creation. Thus, we have not drawn a hard line between the essays John Peter Zenger published and the act of setting the type.

Anderson v. City of Hermosa Beach, 621 F.3d 1051, 1061-62 (9th Cir. 2010).

Thus, the First Amendment protects the right to use a machine to make a recording of an event, which is both the collection and creation of information. Perhaps most famously during this era of increased public concerns about law enforcement misconduct, the First Amendment protects the right to use a mobile phone to record the images and sounds of a police officer performing their official duties. In the words of the Seventh Circuit: "The right to publish or broadcast an audio or audiovisual recording would be insecure, or largely ineffective, if the antecedent act of *making* the recording is wholly unprotected[.]" *ACLU of Illinois v. Alvarez*, 679 F.3d 583, 595 (7th Cir. 2012). Many other courts likewise protect the right to record on-duty police. *Glik v. Cunniffe*, 655 F.3d 78, 82-84 (1st Cir. 2011); *Fields v. City of Philadelphia*, 862 F.3d 353, 359-60 (3d Cir. 2017); *Turner v. Driver*, 848 F.3d 678, 687-90 (5th Cir. 2017); *Askins v. DHS*, 899 F.3d 1035, 1043-44 (9th Cir. 2018); *Smith v. City of Cummings*, 212 F.3d 1332, 1333 (11th Cir. 2000); *State v. Russo*, 141 Hawai'i 181, 190-194 (2017).

Here, faceprinting is both the collection and creation of information. It collects information about the unique shape and measurements of a person's face. And it creates information about that face in the form of a unique representation. Clearview engages in faceprinting for the purpose of later expressing information about its faceprints. That is, Clearview uses its faceprints to provide information to its clients about the people depicted in probe photos. So Clearview's faceprinting enjoys at least some First Amendment protection.

B. Using computer code to generate mathematical representations of faces does not reduce First Amendment protections.

Clearview's use of software to create mathematical representations of faces—the output of its faceprinting—does not reduce the First Amendment protection accorded in this case.

Courts have consistently held that computer code is protected speech. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449 (2d Cir. 2001); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000); *Bernstein v. DOJ*, 176 F.3d 1132, 1141 (9th Cir. 1999), *vacated on other grounds*, 192 F.3d 1308 (9th Cir. 1999). "The fact that a medium of expression has a functional capacity should not preclude constitutional protection." *Junger*, 209 F.3d at 484. Code, like a written musical score, "is an expressive means for the exchange of information and ideas." *Id.* at 485. *See also Corley*, 273 F.3d at 449. Thus, to the extent the application of BIPA to Clearview regulates the code used in Clearview's faceprinting, that code is protected under the First Amendment.

More to the point, the faceprints at issue in this case are not themselves "functional" computer code that can be "run," but rather mathematical representations of biometric identifiers. These representations—the faceprints used by Clearview to identify probe photos—receive First Amendment protection in the same manner as musical scores and other "symbolic notations not comprehensible to the uninitiated." *Corley*, 273 F.3d at 445.

II. The application of BIPA to Clearview's faceprinting is subject to intermediate First Amendment review.

Of course, not all expression warrants the same level of protection. In this case, the applicable test is intermediate judicial review, not strict scrutiny, for two intertwined reasons. First, "speech solely in the individual interest of the speaker and its specific business audience" that concerns "no public issue" warrants "reduced constitutional protection." *Dun & Bradstreet*,

Inc. v. Greenmoss Builders, Inc., . 472 U.S. 749, 762 & n.8 (1985) Second, "expression related solely to the economic interests of the speaker and its audience" is "commercial speech" that receives "lesser protection" compared to "other constitutionally guaranteed expression." *Central Hudson Gas & Electric Corp. v. Public Service Commn.*, 447 U.S. 557, 561, 563 (1980).

Here, Clearview's faceprinting does not concern a public issue, *infra* Part II(A), and it is related solely to Clearview's economic interests, *infra* Part II(B). So the First Amendment requires intermediate review of the application of BIPA's consent requirement to Clearview's faceprinting. This demands a close fit between the means and ends. *Infra* Part II(C).

A. Clearview's faceprinting is not a matter of public concern.

The First Amendment represents a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open." *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964). On the other hand, "where matters of purely private significance are at issue, First Amendment protections are often less rigorous." *Snyder v. Phelps*, 562 U.S. 443, 452 (2011). Accordingly, subject to constitutional safeguards, states can regulate certain purely private speech. *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 345-46 (1974). The Court has applied this rule in many contexts. *See, e.g.*, *Dun & Bradstreet*, 472 U.S. at 757 (defamation); *Snyder*, 562 U.S. at 459 (intentional infliction of emotional distress); *Bartnicki v. Vopper*, 532 U.S. 514, 533 (2001) (wiretapping).

Meanwhile, common law has long recognized torts that limit the collection of truthful private information, such as intrusion on seclusion, or limit its publication, such as public disclosure of private facts. *See* Second Restatement of Torts §§ 652B, 652D.The Supreme Court has "pointedly refused" to hold that the First Amendment categorically precludes liability for such invasions of privacy. *Florida Star v. B.J.F.*, 491 U.S. 524, 533 (1989). It has instead

counseled that "clashes between First Amendment and privacy rights" should be resolved by "rely[ing] on limited principles that sweep no more broadly than the appropriate context of the instant case." *Id. See also Bartnicki*, 532 U.S. at 529 (endorsing case-by-case approach). In *Florida Star*, for example, the Court held that a newspaper could not be punished for publishing the name of a rape victim in violation of a state statute because it had "lawfully obtain[ed]" this truthful information from the government itself, and that the publication concerned a "matter of public significance." 491 U.S. at 536 (quoting *Smith v. Daily Mail Publ'g Co.*, 443 U.S. 97, 103 (1979)). But "[t]o the extent sensitive information rests in private hands, the government may under some circumstances forbid its nonconsensual acquisition." 491 U.S. at 534.

Hence, lower courts have held that privacy torts do not offend the First Amendment as long as they do not restrict important discussion of matters of public concern. *See, e.g.*, *Judge v. Saltz Plastic Surgery, P.C.*, 367 P.3d 1006, 1011 & n.4 (Utah 2016); *Shulman v. Group W Productions, Inc.*, 955 P.2d 469, 479 (Cal. 1998); *Coplin v. Fairfield Pub. Access Television Comm.*, 111 F.3d 1395, 1404 (8th Cir. 1997); *Reuber v. Food Chem. News, Inc.*, 925 F.2d 703, 719 (4th Cir. 1991); *Gilbert v. Med. Econ. Co.*, 665 F.2d 305, 308 (10th Cir. 1981); *Virgil v. Time, Inc.*, 527 F.2d 1122, 1128–29 (9th Cir. 1975). Under a common formulation of the public disclosure tort, "[i]f the contents of a broadcast or publication are of legitimate public concern, the plaintiff cannot establish a necessary element of the tort action." *Shulman*, 955 P. 2d at 479. *See also Judge*, 367 P.3d at 1012 (adopting lack of newsworthiness as an element of public disclosure tort); *Reuber*, 925 F.2d at 719 (publication must not be on a matter of public concern).

The universe of speech that involves matters of public concern is broad, but not unlimited. Whether speech addresses a matter of public concern depends on its "content, form, and context," based on the whole record. *Snyder*, 562 U.S. at 453 (quoting *Dun & Bradstreet*,

472 U.S. at 761). In *Dun & Bradstreet*, a plurality[1] found a defamatory credit report concerned "no public issue" based on several factors: (1) it was "damaging to the victim's business reputation"; (2) it was "solely in the individual interest of the speaker and its specific business audience"; and (3) it was only distributed to a limited number of recipients, paying subscribers who were contractually prohibited from further distribution of the report. 472 U.S. at 761-62.

As with the credit report in *Dun & Bradstreet* and publications that are actionable as privacy torts, Clearview's faceprinting is the relatively unusual case of protected First Amendment activity that serves "no public issue." Clearview extracts faceprints from billions of face photos, absent any reason to think any particular person in those photos will engage in a matter of public concern. Indeed, the overwhelming majority of these people will not engage in matters of public concern in relation to their faceprint. Clearview's sole purpose is to sell the service of identifying people in probe photos, devoid of any journalistic, artistic, scientific or other purpose. It makes this service available to a select set of paying customers. *See Dun & Bradstreet*, 472 U.S. at 761-62. And, similar to the judgment underlying defamation as a viable cause of action in *Dun & Bradstreet*, BIPA represents a considered judgment by the Illinois legislature that faceprinting is damaging to the privacy, speech, and informational security interests of its citizens. *Infra* Part III.

Finally, Clearview's faceprinting does not become a matter of public concern just because the company sells this service to law enforcement agencies. That would prove too much. All personal data might be used to solve crimes, but not all collection of personal data implicates

[1] Five Justices determined that the report did not involve a matter of public concern. *See* 472 U.S. at 762 (1985) (Powell, J., joined by Rehnquist, J. and O'Connor, J); *id.* at 764 (Burger, J., concurring in the judgment) (speech at issue related to a "matter of essentially private concern"); *id.* at 774 (White, J., concurring in the judgment) ("the defamatory publication in this case does not deal with a matter of public importance").

a matter of public concern.

B. Clearview's interests in faceprinting are solely economic.

The Supreme Court defines "commercial speech" as "expression related solely to the economic interests of the speaker and its audience." *Central Hudson Gas*, 447 U.S. at 561, 563.[2]

Thus, when faced with First Amendment challenges to laws that protect consumer data privacy from commercial data processing, courts apply intermediate judicial review under the commercial speech doctrine. *See, e.g.*, *Trans Union Corp. v. FTC* (*Trans Union I*), 245 F.3d 809, 819 (D.C. Cir. 2001) (upholding FTC rule under Fair Credit Reporting Act requiring opt-in consent to sell marketing lists of people based on credit history); *Individual Reference Services Group v. FTC*, 145 F. Supp. 2d 6, 44 n.33 (D.D.C. 2001) (upholding FTC rule under Gramm-Leach-Bliley Act requiring opt-out consent from use and disclosure of "credit header" information such as address, SSN, and phone number); *Trans Union LLC v. FTC* (*Trans Union II*), 295 F.3d 42, 52–53 (D.C. Cir. 2002) (upholding FTC rule under Gramm-Leach-Bliley Act that restricted sharing and use of consumer financial information); *Natl. Cable Assn. v. FCC*, 555 F.3d 996, 1001–02 (D.C. Cir. 2009) (upholding FCC rule under Telecommunications Act requiring opt-in consent to disclose call records to third-party marketers); *King v. Gen. Info. Servs., Inc*., 903 F. Supp. 2d 303, 306-07 (E.D. Pa. 2012) (upholding provision of Fair Credit Reporting Act limiting disclosure of criminal history); *Boelter v. Hearst Inc.* (*Boelter I*), 192 F. Supp. 3d 427, 450–51 (S.D.N.Y. 2016) (upholding state law requiring opt-in consent for a magazine to sell subscribers' data); *Boelter v. Advance Magazine Inc.* (*Boelter II*), 210 F. Supp.

[2] Advertising, *i.e.*, "speech proposing a commercial transaction," is one form of commercial speech. *Central Hudson*, 447 U.S. at 562. There are others. *See, e.g.*, *Greater Philadelphia Chamber of Commerce v. City of Philadelphia*, 949 F.3d 116, 136-39 (2020) (questions from an employer to a job applicant about their salary history).

3d 579, 602 (S.D.N.Y. 2016) (upholding different state law requiring same); *ACA Connects v. Frey*, 471 F. Supp. 3d 318, 331 (D. Me. 2020) (denying motion for judgment on the pleadings against Maine law requiring ISPs to obtain opt-in consent before using or sharing customer data).

Most of these decisions focused not just on the commercial motivation, but also the lack of a matter of public concern. *See, e.g., Trans Union I*, 245 F.3d at 818; *Individual Reference Group*, 145 F. Supp. 2d at 40-41; *Trans Union II*, 295 F.3d 52–53; *King*, 903 F. Supp. 2d at 307; *Boelter I*, 192 F. Supp. 3d at 444-46; *Boelter II*, 210 F. Supp. 3d at 598. *See also Berg v. Merchants Assn.*, 586 F. Supp. 2d 1336, 1344 (S.D. Fla. 2008) (same, as to the Fair Debt Collection Practices Act's limit on phone calls); *Stover v. Fingerhut Marketing*, 709 F. Supp. 2d 473, 478-79 (S.D. W. Va. 2009) (same). *See generally supra* Part II(A).

Here, Clearview has solely economic interests. It amassed a vast trove of billions of faceprints that do not implicate a matter of public concern. Clearview's only purpose is to sell access to information derived from that trove to a select set of clients, rather than the public.

Not to the contrary is *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011), on which Clearview heavily relies, Def. Br. at pp. 14-15. There, the Court struck down Vermont's regulation of how drug company salespersons (known as "detailers") could process prescription information. 564 U.S. at 557. The Court did so because the law discriminated based on speaker and viewpoint. *Id.* at 580. Specifically, the law effectively targeted "detailers—and only detailers," and its "purpose and practical effect" was to "diminish the effectiveness of marketing by manufacturers of brand-name drugs." *Id.* at 564-65. Vermont did this "to tilt public debate" towards generic drugs. *Id.* at 578. The court left the door open to "more coherent" privacy legislation, *id.* at 573, and noted that "[t]he capacity of technology to find and publish personal information … presents serious and unresolved issues with respect to personal privacy and the

dignity it seeks to secure," *id.* at 579. After *Sorrell*, courts still apply *Central Hudson* review to consumer data privacy laws that, like BIPA, do not discriminate based on speaker or viewpoint. *Boelter I*, 192 F. Supp. 3d at 449-50; *King*, 903 F. Supp. 2d at 308–09, 313.

C. Intermediate review requires a close fit between BIPA and Illinois' interests.

To satisfy intermediate review, a speech restraint must "directly advance" and be "narrowly drawn" to a "substantial interest." *Central Hudson*, 447 U.S. at 564-65. This requires "a close fit between ends and means." *McCullen v. Coakley*, 573 U.S. 464, 486 (2014). The speech restriction "must not burden substantially more speech than is necessary to further the government's legitimate interests," though it "need not be the least restrictive or least intrusive means of serving the government's interests." *Id.*

III. Illinois has substantial interests in protecting its residents from faceprinting.

Faceprinting is a special menace to biometric privacy, the freedom of expression that often rests on privacy, and information security. Thus, Illinois has substantial interests in enacting legislation like BIPA that protects residents from faceprinting.

A. Protecting privacy.

Government has a "substantial" interest in promoting consumer data privacy. *Trans Union I*, 245 F.3d at 818; *Natl. Cable*, 555 F.3d at 1001; *King*, 903 F. Supp. 2d at 309–10; *Boelter I*, 192 F. Supp. 3d at 448; *Boelter II*, 210 F. Supp. 3d at 599. "Advances in technology can increase the potential for unreasonable intrusions into personal privacy," *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 599 (9th Cir. 2020), so this interest will grow with time. *Cf. Kyllo v. United States*, 533 U.S. 27, 33–35 (2001) (Fourth Amendment protections must account for "the advance of technology").

Faceprinting poses a special threat to privacy. Individuals expose their faces to public

view every time they go outside. Also, most people have photos accessible online—many of which they did not take or share themselves.[3] Because of easy access to a person's image, faceprinting allows for covert, remote, and mass capture and identification of images.[4]

As the Ninth Circuit recognized in another BIPA case, faceprints can be used to identify an individual in hundreds of millions of other existing photos, "as well as determine when the individual was present at a specific location." *Patel*, 932 F.3d at 1273. Faceprints also allow companies to map relationships among people by identifying others in a photo, such as family, friends, and acquaintances. Also, face-mapped individuals may "be identified from a surveillance photo taken on the streets or in an office building." *Id*. Face surveillance, like location tracking, makes it easy to follow people throughout their lives, including at lawful political protests and other sensitive gatherings, revealing not just "particular movements, but through them … 'familial, political, professional, religious, and sexual associations.'" *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). Therefore, as the Ninth Circuit concluded in *Patel*, "the development of a face template using facial-recognition technology without consent … invades an individual's private affairs and concrete interests." 932 F.3d at 1273.

B. Protecting expression.

Clearview is not the only party whose First Amendment interests are implicated by this case. Illinois has a substantial interest in protecting the free expression that relies on privacy.

The First Amendment protects the rights to confidentially engage in expressive activity,

---

[3] *See, e.g.*, Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. Times (Jan. 18, 2020), https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html (Clearview "returned numerous results, dating back a decade, including photos of myself that I had never seen before").

[4] See Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 Minn. L. Rev. 407, 415 (Dec. 2012).

NAACP v. Alabama, 357 U.S. 449, 460 (1958); to speak anonymously, *McIntyre v. Ohio Elections Commn.*, 514 U.S. 334, 357 (1995); to converse privately, *Bartnicki v. Vopper*, 532 U.S. at 532-33; to confidentially receive unpopular ideas, *Lamont v. Postmaster General*, 381 U.S. 301, 305-307 (1965); and to confidentially gather newsworthy information from undisclosed sources, *Branzburg v. Hayes*, 408 U.S. 665, 709-710 (1972) (Powell, J., concurring). "In a democratic society privacy of communication is essential if citizens are to think and act creatively and constructively. Fear or suspicion that one's speech is being monitored by a stranger . . . can have a seriously inhibiting effect upon the willingness to voice critical and constructive ideas." *Bartnicki*, 532 U.S. at 543.

Faceprinting threatens the First Amendment activities that depend on privacy. Police use it to identify protesters,[5] including with Clearview's help.[6] Police can also use it to identify who attended a protest planning meeting, who visited an investigative reporter, who went to a controversial movie, and who distributed an unsigned pamphlet. This will chill speech.

C. Protecting information security.

Illinois has a substantial interest in protecting the information security of its residents. Data thieves regularly steal vast troves of personal data.[7] If a faceprint database is breached, then

---

[5] James Vincent, *NYPD used facial recognition to track down Black Lives Matter activist*, The Verge (Aug. 18, 2020), https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

[6] Connie Fossie and Phil Prazan, *Miami Police Used Facial Recognition Technology in Protester's Arrest*, NBC Miami (Aug. 17, 2020), https://www.nbcmiami.com/investigations/miami-police-used-facial-recognition-technology-in-protesters-arrest/2278848/.

[7] Tara Siegel Bernard, et al., *Equifax Says Cyberattack May Have Affected 143 Million in the U.S.*, N.Y. Times (Sept. 7, 2017), https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html; Erik Ortiz, *Marriott Says Breach of Starwood Guest Database Compromised Info of Up to 500 Million*, NBC News (Nov. 30, 2018), *available at* https://www.nbcnews.com/tech/security/marriott-says-data-breach-compromised-info-500-million-guests-n942041.

criminals and foreign governments can use stolen faceprints to break into secured accounts that can be opened by the owner's face. Indeed, a team of security researchers used Facebook photos to build 3D models that could fool facial recognition security systems.[8]

IV. BIPA's consent requirement, as applied to Clearview's faceprinting, is narrowly drawn to Illinois' substantial interests.

There is a "close fit," *McCullen*, 573 U.S. at 486, between (i) Illinois' substantial interests in protecting its residents' biometric privacy, free speech, and information security, and (ii) BIPA's requirement that Clearview obtain opt-in consent before collecting a person's faceprint. Information privacy requires "the individual's control of information concerning [their] person." *DOJ v. Reporters Committee*, 489 U.S. 749, 763 (1989). *See also Natl. Cable*, 555 F.3d at 1001 ("privacy deals with determining for oneself when, how, and to whom personal information will be disclosed to others"). Illinoisans have lost control over their faceprints, and BIPA precisely solves this problem by restoring their control. Doing so does not "burden substantially more speech than is necessary." *McCullen*, 573 U.S. at 486.

Numerous courts have upheld, against First Amendment challenges, laws requiring opt-in consent to process personal data. *See, e.g.*, *Natl. Cable*, 555 F.3d at 1001–02; *Trans Union I*, 245 F.3d at 819; *Boelter I*, 192 F. Supp. 3d at 450–51; *Boelter II*, 210 F. Supp. 3d at 602. Many other data privacy laws require opt-in consent to process a person's data. *E.g.*, 47 U.S.C. §§ 551(b)(1) & (c)(1) (cable); 18 U.S.C. § 2710(b)(2) (videos); 47 U.S.C. § 222 (telecommunications).

Courts reject the argument that opt-in consent fails intermediate review because it is more burdensome for businesses than an opt-out scheme. Opt-out is only "marginally less intrusive,"

[8] *3D models based on Facebook images can fool facial recognition systems*, Cyber Defense Mag. (Aug. 25, 2016), https://www.cyberdefensemagazine.com/3d-models-based-on-facebook-images-can-fool-facial-recognition-systems/.

Nat'l Cable, 555 F.3d at 1002, and thus does not void the rule, *Boelter I*, 192 F. Supp. 3d at 450. Under intermediate review, a legislature "ha[s] no obligation to choose the least restrictive means of accomplishing its goal." *Trans Union I*, 245 F.3d at 819. *See also Boelter II*, 210 F. Supp. 3d at 602 (the restraint need not be "absolutely the least severe that will achieve the desired end").[9]

Moreover, opt-out consent is not an effective way to protect people from faceprinting. Many won't know a business collected their faceprint at a distance or from photos. Many more won't know they have the right to opt-out or how to do so. Still more will be deterred because the process is time-consuming, confusing, or frustrating.[10] Indeed, many companies purposefully deploy "dark patterns" that trick users into submitting to data processing.[11] This is one reason so few people change their privacy defaults.[12] So there is the requisite "close fit," *McCullen*, 573 U.S. at 486, between Illinois' opt-in consent requirement and its substantial interests.

CONCLUSION

For the foregoing reasons, amicus EFF respectfully requests that this Court reject Clearview's First Amendment defense and deny its motion to dismiss.

---

[9] These four cases did not follow *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999), which erroneously held that opt-out is an adequate substitute for opt-in. As the dissent explained, opt-out "does not guarantee that a customer will make an informed decision," and "creates the very real possibility of 'uninformed' customer approval." *Id.* at 1246-47.

[10] A Consumer Reports study found that "[m]any data brokers' opt-out processes are so onerous that they have substantially impaired consumers' ability to opt out …" Maureen Mahoney, *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* (Oct. 1, 2020), https://advocacy.consumerreports.org/wp-content/uploads/2020/09/CR_CCPA-Are-Consumers-Digital-Rights-Protected_092020_vf.pdf.

[11] Alexis Hancock, *Designing Welcome Mats to Invite User Privacy*, EFF Deeplinks (Feb. 14, 2019), https://www.eff.org/deeplinks/2019/02/designing-welcome-mats-invite-user-privacy-0.

[12] Charles Arthur, *Why the default settings on your device should be right the first time*, The Guardian (Dec. 1, 2013), https://www.theguardian.com/technology/2013/dec/01/default-settings-change-phones-computers; Markus Tschersich, *Comparing the Configuration of Privacy Settings on Social Network Sites Based on Different Default Options* (2015), https://www.computer.org/csdl/pds/api/csdl/proceedings/download-article/12OmNzvhvLe/pdf.

Date: July 9, 2021

Respectfully submitted:

/s/ Adam Schwartz

Adam Schwartz
Jennifer Lynch
Electronic Frontier Foundation
815 Eddy St.
San Francisco, CA 94109
415.436.9333
adam@eff.org
jlynch@eff.org

Counsel for amicus EFF

CERTIFICATE OF SERVICE

I certify that on July 9, 2021, I filed the foregoing document electronically with the clerk of the court for the Northern District of Illinois, Eastern Division, using the CM/ECF system which causes a copy to be delivered by email to all counsel of record in this case.

/s/ Adam Schwartz
Adam Schwartz